UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/465,514	12/16/1999	HENRY M. GLADNEY	A7254	8969

46159 7590 05/31/2007

SUGHRUE MION PLLC
USPTO CUSTOMER NO WITH IBM/SVL
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/465,514	GLADNEY, HENRY M.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *27-33* is/are pending in the application.

4a) Of the above claim(s) *1-26 and 34-46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *27-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 27-33 are pending.

Claims 1-26 and 34-46 are cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **3/14/2007** has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 27-33 are rejected under 35 U.S.C. 102(e) as being anticipated by He, et al. (US 6,088,451).

As per claim 27:

An information storage management system in a first administrative domain administered by a first organization, comprising:

a collection of stored objects; **(col.1, lines 11-16 and col.6, lines 20-57; He discloses network elements are considered individual systems that provide services to users that lead to access to valuable system resources and information in the elements (col.4, lines 7-10). He discloses network resources and information reside in various network elements such as mainframe computer or database servers. Thus, the resources and information is the claimed stored objects (col.1, lines 11-16). He further discloses the central theme around security of network elements is how user access can be appropriately and effectively controlled for access to network elements. Total blocking of access to network elements does not serve the purpose of resource and information sharing between users and systems or access without any control exposes the network elements to abuse and subject to malicious attacks that could result in the disclosure of sensitive information (col.5, lines 5-19). Thus, He discloses the network elements provide valuable network resources and information to legitimate users where access to network elements must be properly screened to prevent, to limit, and to detect illegitimate activities (col.6, lines 21-28). User identification through the assignment of a unique system wide identifier provides necessary means for the identification of legitimate users (col.8, lines 13-35). Hence, the resources and information residing in the network elements are**

protected and limited to legitimate user access is referring to the claimed collection of stored objects and also to the claimed determining if a requestor is authorized to access a protected object stored in the collection (col.6, lines 21-23 and col.8, lines 15-20).)

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection; **(col.8, lines 13-40 and col.18, lines 10-11; the claimed access control unit is the local access control system (LACS).)**

a resource manager connected to the access control unit and to a communications channel; **(col.2, lines 30-35 and col.14, lines 18-22; He discloses the claimed resource manager as the local access control means is an interface that is provided at each user element. He discloses the user element is the interface to users for access to network resources and information (col.7, lines 4-6). The user element is for managing access to resources and thus, reads on a resource manager.)**

wherein the resource manager receives a user's request for access to the protected object **(col.9, lines 48-52 and col.17, lines 55-60)**, the request including a globally unique identifier for the user requesting the access **(col.8, lines 22-23 and col.16, lines 27-29)**, and in response to the user's request, the resource manager sends over the communications channel **(col.32, lines 28-39)** to an external storage management system **(col.2, lines 24-29 and col.12, lines 53-55)** in a second administrative domain administered by a second organization that is different from the first organization **(col.14, lines 39-58 and col.30, lines 54-60; He discloses a network**

security server (NSS) that includes the authentications server (access control unit), credential server, and network element access server (col.11, lines 34-59). The authentication server of the NSS is responsible for determining the authentication of the users or requestors and includes a database of user information. Hence, the external storage management system involves the NSS and the registration database (col.2, lines 13-29 and col.12, lines 53-55). He discusses that each sub-network is called a realm and is an independent administrative entity where each realm have its own set of network security servers (col.14, line 63-col.15, line 2). He further suggests access to network resources and information that are in a network element 104 in a different realm 302 than the current one through a mechanism called inter-realms authentication. Each realm can have their own registration database (col.15, lines 13-21). He discloses access to network resources and information controlled from both local and remote user access (col.1, lines 65-67). Thus, He suggests different other external storages in different other administrative domains administered by different other organization.), a resource manager request for information about the user, the resource manager request including the globally unique identifier; and **(col.8, lines 13-34 and col.16, lines 30-67; He discloses the network-wide unique identifier as the claimed globally unique identifier.)**

wherein the resource manager upon receiving a response to the resource manager request **(col.13, lines 52-63 and col.17, lines 62-66)** from the external storage management system passes the user information to the access control unit;

and **(col.18, lines 2-12; The registration database keeps user account information for the control decision to make decisions for the user, hence this information is given in response to the request for access to the network resources and information (col.16, lines 44-46).)**

wherein responsive to the user information the access control unit determines whether to authorize the user for access to the protected object. **(col.18, lines 24-31 and col.28, lines 9-13; the LACS (access control unit) certify the user credential, which was included with the user information sent as a ticket with a key.)**

As per claim 28: see col.8, lines 21-23 and col.16, lines 28-30 and 44-46; discussing the subject identifier is a Universal Unique Identifier (UUID).

As per claim 29: see col.8, lines 13-34 and col.16, lines 28-67; discussing the user information is organization information indicating whether the user is a member of an organization.

As per claim 30:

An information storage management system in a first administrative domain administered by a first organization, comprising:

a collection of stored objects; **(col.1, lines 11-16 and col.6, lines 20-57; He discloses network elements are considered individual systems that provide services to users that lead to access to valuable system resources and information in the elements (col.4, lines 7-10). He discloses network resources and information reside in various network elements such as mainframe computer**

or database servers. Thus, the resources and information is the claimed stored objects (col.1, lines 11-16). He further discloses the central theme around security of network elements is how user access can be appropriately and effectively controlled for access to network elements. Total blocking of access to network elements does not serve the purpose of resource and information sharing between users and systems or access without any control exposes the network elements to abuse and subject to malicious attacks that could result in the disclosure of sensitive information (col.5, lines 5-19). Thus, He discloses the network elements provide valuable network resources and information to legitimate users where access to network elements must be properly screened to prevent, to limit, and to detect illegitimate activities (col.6, lines 21-28). User identification through the assignment of a unique system wide identifier provides necessary means for the identification of legitimate users (col.8, lines 13-35). Hence, the resources and information residing in the network elements are protected and limited to legitimate user access is referring to the claimed collection of stored objects and also to the claimed determining if a requestor is authorized to access a protected object stored in the collection (col.6, lines 21-23 and col.8, lines 15-20).)

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection; **(col.18, lines 10-11; the claimed access control unit is the local access control system (LACS).)**

a resource manager connected to the access control unit and to a communications channel; **(col.2, lines 30-35 and col.14, lines 18-22 and col.32, lines 28-39); He discloses the claimed resource manager as the local access control means is an interface that is provided at each user element. He discloses the user element is the interface to users for access to network resources and information (col.7, lines 4-6). The user element is for managing access to resources and thus, reads on a resource manager.)**

wherein the resource manager receives a user's request for access to the protected object **(col.9, lines 48-52 and col.17, lines 55-60)**, the request including a globally unique identifier for the user requesting the access **(col.8, lines 22-23 and col.16, lines 27-29)**, and in response to the user's request the resource manager resolves the globally unique identifier to a user identifier recognized by an external storage management system **(col.2, lines 24-29 and col.12, lines 53-55)** in a second administrative domain administered by a second organization that is different from the first organization **(col.14, lines 39-58 and col.30, lines 54-60; He discloses a network security server (NSS) that includes the authentications server (access control unit), credential server, and network element access server (col.11, lines 34-59). The authentication server of the NSS is responsible for determining the authentication of the users or requestors and includes a database of user information. Hence, the external storage management system involves the NSS and the registration database (col.2, lines 13-29 and col.12, lines 53-55). He discusses that each sub-network is called a realm and is an independent**

administrative entity where each realm have its own set of network security servers (col.14, line 63-col.15, line 2). He further suggests access to network resources and information that are in a network element 104 in a different realm 302 than the current one through a mechanism called inter-realms authentication. Each realm can have their own registration database (col.15, lines 13-21). He discloses access to network resources and information controlled from both local and remote user access (col.1, lines 65-67). Thus, He suggests different other external storages in different other administrative domains administered by different other organization.),; the resource manager sending to the external storage management system a resource manager request for information about the user **(col.8, lines 13-34)**, the resource manager request including the resolved user identifier; and **(col.15, lines 3-4 and col.16, lines 30-67; He discloses the network-wide unique identifier as the claimed globally unique identifier and a name server for pseudo-naming scheme such as to resolve to user identifier (col.15, lines 6-8).)**

wherein the resource manager upon receiving a response to the resource manager request **(col.13, lines 52-63 and col.17, lines 62-66)** from the external storage management system passes the user information to the access control unit; and **(col.18, lines 2-12; The registration database keeps user account information for the control decision to make decisions for the user, hence this information is given in response to the request for access to the network resources and information (col.16, lines 44-46).)**

wherein responsive to the user information the access control unit determines whether to authorize the user for access to the protected object. **(col.18, lines 24-31 and col.28, lines 9-13; the LACS (access control unit) certify the user credential, which was included with the user information sent as a ticket with a key.)**

As per claim 31: see col., lines; discussing the subject identifier is a Universal Unique Identifier (UUID).

As per claim 32: see col.8, lines 21-23 and col.16, lines 28-30 and 44-46; discussing the user information is organization information indicating whether the user is a member of an organization.

As per claim 33: see col.8, lines 13-34 and col.15, lines 3-8 andcol.16, lines 28-67; discussing the resource manager resolves the globally unique identifier by using a name server.

Response to Arguments

4. Applicant's arguments with respect to claims 27-33 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100